

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*INFORMATION ASSOCIATED WITH
MUSALOTTATRUCKS173@GMAIL.COM AND
SMARTFIT173@GMAIL.COM THAT IS STORED AT
PREMISES CONTROLLED BY GOOGLE LLC

Case No. 4:23 MJ 7436 SPM

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. Section 1349
18 U.S.C. Section 1543
18 U.S.C. Section 1028A

Offense Description

Bank Fraud Conspiracy
Use of False Passport
Aggravated Identity Theft

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

jason r fatchett

Digitally signed by jason r fatchett

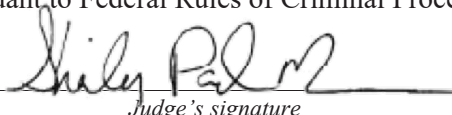
Date: 2023.12.19 16:20:37 -06'00'

Applicant's signature

Jason Fatchett, Special Agent, U.S. Department of State

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 12/20/2023City and state: St. Louis, MO

Judge's signature

Honorable Shirley P. Mensah, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH) No. 4:23 MJ 7436 SPM
MUSALOTTATRUCKS173@GMAIL.COM)
AND SMARTFIT173@GMAIL.COM THAT) FILED UNDER SEAL
IS STORED AT PREMISES CONTROLLED)
BY GOOGLE LLC)

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason Fatchett, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), as well as Federal Rule of Criminal Procedure 41, for information associated with certain accounts, which information is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 (“Google”). The information to be searched is described in the following paragraphs and in **Attachment A**. The search warrant would require Google to disclose to the United States copies of the information (including the content of communications) further described in **Attachment B**. Upon receipt of the information described in Section I of **Attachment B**, United States-authorized persons will review that information to locate the items described in Section II of **Attachment B**.

2. I have been a Special Agent with the United States Department of State, Bureau of Diplomatic Security (“DS”) since 2013 and am currently assigned to the DS Resident Office in St. Louis, Missouri. As a Special Agent with DS, I am responsible for investigating violations of federal law, including Title 18 offenses involving, among other things, passport and visa fraud. During these investigations, I have planned, led, and participated in the execution of search

warrants, arrest warrants, and witness and suspect interviews, have assisted during judicial proceedings, and have performed other, related duties.

3. The facts included in this affidavit come from my personal knowledge and observations, my training and experience, my collection of statements and information from witnesses and other law enforcement officers, and my review of records, documents, and other evidence obtained during this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts included in this affidavit, there is probable cause to believe that violations of federal law, including, but not limited to, violations of 18 U.S.C. § 1349 (bank fraud conspiracy), 18 U.S.C. § 1543 (use of false passport), and 18 U.S.C. § 1028A (aggravated identity theft), have been committed by Michael Grodner (“**Grodner**”), Anthony Ramos (“**Ramos**”), and Ruben Viruet-Stevens (“**Viruet-Stevens**”), as well as other persons known and unknown, including persons using the **Subject Accounts** (defined below). There is also probable cause to search the location described in **Attachment A** for evidence, instrumentalities, contraband, and/or fruits of these crimes, as described in **Attachment B**.

LOCATION TO BE SEARCHED

5. The location to be searched is:

MUSALOTTATRUCKS173@GMAIL.COM (“**Subject Account #1**”), and

SMARTFIT173@GMAIL.COM (“**Subject Account #2**”) (together with **Subject Account #1**, the “**Subject Accounts**”).

Each of the **Subject Accounts** is located at premises controlled by Google, which is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, as further described in **Attachment A**. The items to be reviewed and seized from each of the **Subject Accounts** are described in **Attachment B**.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING GOOGLE

7. Through my training and experience, I have learned the following about Google:

a. Google offers email services to the public. Google allows subscribers to maintain email accounts, such as the **Subject Accounts**, under the domain name gmail.com. A subscriber using Google’s services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber’s account, or stored in draft form in the account, is maintained on Google’s servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google’s computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google’s servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet Protocol (“IP”) address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber’s means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Android ID, Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the

user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's websites). Google also retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

viii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from law enforcement pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

8. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, including the following:

a. *Google Drive content.* Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud" (*i.e.*, online). A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet.

Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

c. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photographs and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data and can include GPS location information for where a photograph or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which events are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions called “Hangouts,” which permit the sharing of additional content such

as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

f. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications ("apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile.* Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus.* Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply "friends") into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user's Circle having previously clicked "+1" next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user's Circle.

j. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes

information about websites viewed by the user and Internet search queries in the Google Internet search engine available at <http://www.google.com> (and variations thereof, including <http://www.google.ru>), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

k. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

l. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user.

9. Therefore, the computers of Google and are likely to contain stored electronic communications (including retrieved and unretrieved email) for Google subscribers and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

10. As explained above, Google subscribers can also store files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

11. In my training and experience, Google generally asks its subscribers to provide certain personal identifying information when registering for an email account. Such information

can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

12. In my training and experience, in some cases, email account users will communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers like Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

13. In short, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who

used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, email providers, including Google, typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crimes under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account subscriber. Additionally, information stored on the user's account may further indicate the geographic location of the user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the account subscriber's state of mind as it relates to the offenses under investigation. For example, information in the email account may indicate the user's motive and intent to commit a crime (*e.g.*, communications relating to the crimes), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE

14. DS has been investigating numerous incidents of bank fraud, use of false passports, and identity theft that occurred in multiple jurisdictions, including an incident involving **Grodner**, **Ramos**, and **Viruet-Stevens** that occurred within the Eastern District of Missouri on March 16, 2023.

15. Specifically, on March 16, 2023, **Grodner**, **Ramos**, and **Viruet-Stevens** were arrested by the Maryland Heights (Missouri) Police Department ("MHPD") after **Grodner** attempted to deposit a fake check into a business's account at UMB Bank by using a fake United

States passport card that contained the true name and birthdate of the business's owner but displayed a photograph of **Grodner**.



16. When **Grodner**, **Ramos**, and **Viruet-Stevens** were arrested, they were occupying a Dodge Charger. **Grodner** was found in possession of, among other items, three additional fake United States passport cards (each of which contained the true name and date of birth of another individual but displayed a photograph of **Grodner**), as well as a Delta Boarding pass for a March 16, 2023 flight from New York to St. Louis. **Ramos** was found seated next to five additional fake checks. **Viruet-Stevens** was found seated next to an Enterprise Rent-A-Car (“Enterprise”) rental agreement, which showed that the Dodge Charger had been rented from Enterprise earlier that day.

17. Following their arrest, **Grodner**, **Ramos**, and **Viruet-Stevens** were each separately interviewed by MHPD and DS (after they were each verbally advised of and indicated that they understood their *Miranda* rights). During their interviews, **Ramos** and **Viruet-Stevens** disclosed that their flights to St. Louis were arranged and paid for by a person who they know as “**TJ**.” While **Grodner** disclosed only that his flight was arranged and paid for by a guy from New York, a subsequent search of his phone (pursuant to a court-authorized search warrant) revealed text message communications between him and **TJ**, who was using the phone number (845) 546-9592

(the “**9592 Phone Number**”), including a March 16, 2023 text message communication in which TJ wrote “I bought tickets and you shut your phone off and fucked me.”

18. Investigators thereafter conducted further investigation to identify **TJ**, as well as any other persons who were part of the above-referenced scheme involving **Grodner, Ramos, and Viruet-Stevens**. Evidence obtained during the investigation indicated that **TJ** and/or such other persons used the **Subject Accounts** in furtherance of the scheme.

19. Investigators obtained records and video footage from Enterprise relating to the March 16, 2023 rental of the Dodge Charger. Enterprise’s records reflected that the Dodge Charger was rented under the name Mohamed Ifthikar (“**Ifthikar**”), whose phone number was listed as the **9592 Phone Number** and whose email address was listed as smartfit173@gmail.com (*i.e.*, **Subject Account #2**). Investigators compared **Ifthikar’s** passport photograph, which was obtained from a law enforcement database, to the person who rented the Dodge Charger as shown on Enterprise’s video footage, and determined that the person on the video footage did not match **Ifthikar’s** passport photograph.

20. Investigators subpoenaed records from Delta relating to **Grodner, Ramos, and Viruet-Stevens**. Delta’s records reflected that:

a. The March 16, 2023 flights that **Grodner, Ramos, and Viruet-Stevens** took from New York to St. Louis were booked online under **Ifthikar’s** name using the email address musalottatrucks173@gmail.com (*i.e.*, **Subject Account #1**) and listing the **9592 Phone Number** in the contact information section;

b. The electronic device on which the flights were booked used the IP address 24.186.183.226 (the “**New York IP Address**”); and

c. A fourth traveler named Fritz Oslin (“**Oslin**”) flew with **Grodner**, **Ramos**, and **Viruet-Stevens** from New York to St. Louis on March 16, 2023.

21. Delta’s records further reflected that other flights were booked for **Grodner** and/or **Ramos** (among other persons) using the email address smartfit173@gmail.com (*i.e.*, **Subject Account #2**) and listing the **9592 Phone Number** in the contact information section. These flights included, but were not limited to, a February 10, 2023 flight from Milwaukee, Wisconsin to New York, which flight coincided with two other bank fraud/identity theft incidents that occurred in Wisconsin on February 10, 2023 for which **Grodner** is a suspect and in which **Ramos** is believed to have participated:

a. *February 10, 2023 in Wales, Wisconsin:* **Grodner** went into a Town Bank branch, deposited a \$4,500 fake check into a business’s account, and then impersonated the business’s owner to immediately withdraw \$6,200 from the account.

Digital Video Snapshot

Recorder: Town - Wales - MNAR1539V226
Camera Name: TELLER 2



b. *February 10, 2023 in Oconomowoc, Wisconsin:* **Grodner** went into an Ixonia Bank branch, deposited a \$4,500 fake check into a business's account, and then used a fake United States passport card containing the name of the business's owner to immediately withdraw \$6,000 from the account.



22. Investigators also obtained a search warrant for the email address smartfit173@gmail.com (*i.e.*, **Subject Account #2**), which was the email address that was listed on Enterprise's records for the rental of the Dodge Charger in St. Louis and that was used to book **Grodner's** and **Ramos's** February 10, 2023 flights from Milwaukee to New York. Records produced by Google pursuant to the search warrant (which records only went through May 2023 because that is when the search warrant was obtained) contained evidence indicating, among other things, that, as of early 2023, the person using **Subject Account #2** was residing at 104 Town Green Drive, Elmsford, New York 10523 (and using the **9592 Phone Number**), including because merchandise ordered online was shipped to that address, numerous Lyft rides were purchased to and from that address, emails from the service provider for the **New York IP Address** included that address in the "account information" details, and numerous other emails referenced that

address (as well as the **9592 Phone Number**). These records also contained evidence demonstrating that, between December 2022 and March 2023, **Subject Account #2** was used to book numerous flights to destinations across the United States for 11 different people, including **Grodner, Ramos, and Oslin** (who flew together to St. Louis on March 16, 2023).

23. Investigators also subpoenaed information from Google relating to the email address musalottatrucks173@gmail.com (*i.e.*, **Subject Account #1**), which was the email address used to book the March 16, 2023 St. Louis flights for **Grodner, Ramos, Viruet-Stevens, and Oslin**. This information reflected that **Subject Account #1** used the **New York IP Address** multiple times between March 2023 and July 2023, and that the name listed for the subscriber of **Subject Account #1** was “Musa Nyakako.” When that name was cross-referenced with the records produced by Google pursuant to the search warrant for **Subject Account #2**, investigators discovered that there were more than 100 emails addressed to that name. In addition, when **Subject Account #1** was cross-referenced with Delta’s records, Delta’s records reflected that **Subject Account #1** was previously used to book multiple flights for **Ramos** (among other persons) in 2022 (in addition to the March 16, 2023 flight to St. Louis).

24. On December 15, 2023, I submitted a preservation request to Google requesting that Google preserve records associated with each of the **Subject Accounts**. That same day, Google confirmed that it was preserving records associated with each of the **Subject Accounts**.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it,

reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

26. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.


I state under the penalty of perjury that the foregoing is true and correct.

jason r fatchett

Digitally signed by jason r
fatchett
Date: 2023.12.19 16:19:40 -06'00'

Jason Fatchett
Special Agent
United States Department of State,
Bureau of Diplomatic Security

**Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to
Federal Rules of Criminal Procedure 4.1 and 41 on December 20, 2023.**


SHIRLEY P. MENSAH
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with:

MUSALOTTATRUCKS173@GMAIL.COM (“**Subject Account #1**”), and

SMARTFIT173@GMAIL.COM (“**Subject Account #2**”) (together with **Subject Account #1**, the “**Subject Accounts**”),

which information is stored at premises owned, maintained, controlled, or operated by Google LLC (“**Google**”), whose headquarters is located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in **Attachment A** is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on December 15, 2023, Google is required to disclose the following information, for the time period of **July 1, 2022 to the present**, to the United States for each account or identifier listed in **Attachment A**:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification and subscriber of the account, including, but not limited to, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All location history data;

d. All advertising data;

- e. Full Google search history and Chrome browser history associated with the account;
- f. All services used by the account;
- g. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- h. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken;
- i. All billing and payment information;
- j. All past and current usernames, account passwords, and names associated with the account;
- k. All YouTube data associated with the account;
- l. All information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;
- m. All activity logs for the account;
- n. All photos and videos uploaded to the account, including in Google Drive and Google Photos;

- o. All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;
- p. All photos and videos uploaded by any user that have the account user tagged in them;
- q. All location and maps information;
- r. All Google Voice information;
- s. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- t. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;
- u. All accounts linked to the account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);
- v. For accounts linked by cookie, the date(s) on which they shared a cookie;
- w. For accounts linked by SMS number, information regarding whether the numbers were verified; and
- x. All cookies associated with or used by any computer or web browser associated with the account, including the IP addresses, dates, and times associated with the recognition of any such cookie.

The Provider is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 1349 (bank fraud conspiracy), 18 U.S.C. § 1543 (use of false passport), and 18 U.S.C. § 1028A (aggravated identity theft) from July 1, 2022 to the present, including, for each account or identifier listed on **Attachment A**, information pertaining to the following matters:

- (a) Evidence relating in any way to bank fraud, use of false passports, and/or identity theft;
- (b) Evidence relating in any way to flights;
- (c) Evidence relating in any way to rental car reservations and/or rental car rental agreements;
- (d) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner and/or user;
- (e) Evidence indicating the account owner's and/or user's state of mind as it relates to the crimes under investigation;
- (f) The identity of the person(s) who created and/or used the account, including records that help reveal the whereabouts of such person(s); and
- (g) The identity of the person(s) who communicated with the account owner and/or user about matters relating in any way to bank fraud, use of false passports, and/or identity theft, as well as activities in furtherance thereof, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature